## REMARKS

By this response, claims 1-58 and 90-101 are pending as a continuing application under 37 C.F.R. §1.114 (Request for Continued Examination (RCE)). Compared to prior versions, claims 1, 20, 49, 50, 90 and 98 are amended while claims 2 and 59-89 are canceled. All others remain as originally or previously presented. To the extent the prior art remains relevant, these remarks address the merits of the Final Office Action mailed April 19, 2005 and the Advisory Action mailed June 13, 2005.

According to the Examiner, all claims stand rejected under 35 U.S.C. §103(a) as obvious in view of the combination of Chang U.S. 6,157,953 and Van Dyke U.S. 6,412,070. It is suggested that Chang includes all the elements of the independent claims with the exception that Van Dyke (relative to claims 1-58) incorporates "having access rights granted to a system administrator, operable to be shared with other users having' [sic] other profiles accessible and administered exclusively by the other users, the string occurring exclusively upon initiation by the user." *Underlining added, Page 4, 1st ¶, 4-19-05 Final Rejection.* Relative to claims 90-101, the Examiner contends Van Dyke supplies the missing teaching by "having access rights granted to one or more system administrators including management of one or more accounts of end users, the one or more safes of digital identities having access rights granted exclusively to the end users via the one or more accounts including the exclusion of access rights of the one or more system administrators." *Page 15, 1st ¶, 4-19-05 Final Rejection.*

Preliminarily, the Applicant would again like to point out that pending claim 1 has no instance of usage of the term "the string" as the Examiner has made reference to in both his final rejection and advisory action. As presently presented, claim 1 recites (in its entirety):

> 1. (Currently Amended) A computer server system for managing digital identity information, comprising at least one

> processor in operable connection with a memory configured by a database, the database including a vault for storage of ~~at least one~~ multiple user objects for [[a]] multiple users, the vault having access rights granted to a system administrator for management of the multiple user objects, each of the user objects having a corresponding safe object, the safe object containing ~~at least one~~ multiple profiles accessed and administered exclusively by a single one of the multiple users at the exclusion of the system administrator, each profile including digital identity information provided by the single one of the multiple users and operable to be shared with other of the multiple users having other multiple profiles accessible and administered exclusively by the other of the multiple users, ***the sharing*** occurring exclusively upon initiation by the single one of the multiple users.

As seen in bold-italics, the claim term is properly "the sharing," not "the string," and it is "the sharing" of digital identity information which "occur[s] exclusively upon initiation by the single one of the multiple users." It is believed the Patent Office made a mistake during its optical scanning of the pending claims and the Applicant respectfully requests reconsideration in view of this mistake. The Applicant does not believe anyone could have made a proper examination of the claim when the term "the string" and "the sharing" have radically different meanings and both greatly alter the meaning of the term "occurring exclusively upon initiation by the single one of the multiple users" that follows thereafter.

Substantively, Chang generally concerns itself with system administrators and their ability to effectively "manag[e] software applications and services from a central location in a computer network." *Emphasis Added, col. 5, ll. 14-15.* In all embodiments, the central location resides on a "server side" of the network, separate and distinct from the ultimate end-users of the network. As borne out in Figure 2, for example, Chang teaches a "server-side configuration 200" having sections 202 and 204 representing "an administrative side" and "network servers, or service hosts," respectively. *Col. 5, l. 67 - col. 6, l. 2.* However,

end users are "[n]ot shown" in the figure and, as distinguished from the server-side, exist "on client machines which can typically access network servers 206 [of the server-side] to provide services or for running applications, or performing other network operations." *Col. 6, ll. 2-5.* To tightly control access of the software applications and authenticate a system administrator's right to manipulate software on the server-side of the network, Chang contemplates an authentication process from a single point-of-control, or central location, as described with regard to Figures 8a and 8b at *col. 12, l. 59, et. seq.*

With more specificity, Chang's authentication process begins at step 802 with an administrator pointing the "the browser host (i.e. administration console 216 of FIG. 2) to a URL of the management console host." At step 804, "the administrator/user is challenged for a user name and password for access to the management console program on the console host. At step 806 the management console accepts the user name and password entered in step 804 and the user is authenticated." *Col. 13, ll. 3-7.* At step 808, the administrator selects services of the various hosts they want to manage. In steps 810, 812 and 814, authentication of the administrator occurs. If authentication is ultimately successful, "the management console program on the console host," e.g., the central location, enables the administrator to "perform management operations on the selected service or services from the browser [216] as shown at step 816 at which point the enforcement process is complete." *Col. 13, ll. 58-62.* In other words, an administrator logs on and becomes authenticated for various service hosts all while being physically located at the centrally-located, web browser host 216. They then perform necessary operations for the service hosts after authentication is complete.

Bear in mind, Chang attempts to overcome prior art problems (*Col. 2, ll. 26-42*) where multiple system administrators, each with varying degrees of authority, need to perform many operations, functions, routines, etc. at multiple locations, including routinely

having to "re-authenticate every time" they sign on to a service host, especially in networks where the multiple "service hosts are not in communication with each other." *Col. 2, ll. 54-56.* As Chang further describes it, this is "inefficient and repetitive." *Col. 2, l. 45.*

In one embodiment, particularly cited by the Examiner in rejecting the user object having a corresponding safe object aspect of claim 1, for example, Chang teaches a "user profile data repository" that "stores data relating to user privileges [of an administration server], including a user access level, a list of services and a password." *Col. 4, ll. 13-15.* ***In this regard, however, a single profile for a single administrator (including access level, a list of services and a password) is stored in memory of an administrative server.*** Naturally, as Chang relates to more than one administrator, each administrator has their own profile for user access, a list of services and password stored in memory of the server.

The instant claims, however, require the notion of 1) multiple profiles of multiple users being shared amongst one another upon user initiation; 2) each of the multiple profiles being stored in safes; 3) each of the safes being stored in vaults; 4) access rights of the vault going to a system administrator to manage the safes in the vaults; and 5) access and administration rights of the multiple profiles of underlying data in the safes, managed by the system administrator, going exclusively to the end users at the exclusion of the system administrator. Unequivocally, Chang never discloses multiple profiles of a single user, sharing of profiles between the multiple users, and sharing of profiles upon user initiation, to name a few.

Van Dyke, however, does not supply the missing teaching. According to Van Dyke, "***control access rights do not control access to data within objects 125***, but control access to an operation, or action, to be performed on or by object 125." *Col. 5, ll. 42-44.* In other words, when Van Dyke teaches the granting of a control access right of an object to another party, according to Figure 7 and *col. 10, ll. 6-19*, for example, as the Examiner cites, it does

not and cannot ever include the party's ability to access the underlying data of the object. It simply grants control of an operation or action to be performed on or by the object. By Van Dyke's very definition, it never gives another party access to the object's data. In turn, Van Dyke fails as a reference in rejecting the claims.

If you combine Van Dyke's granting of a control access right of an object to a third party with Chang's single administrator profile in the administrative server, it will simply enable the third party to manipulate the profile, such as by replicating it, for instance. Conversely, the third party will indefinitely avoid getting access to the actual password data in the profile. The instant invention, on the other hand, provides the opposite. As claimed, various end users actually obtain the underlying data of another end user upon the sharing of a profile. *See, e.g., digital identity information in Applicant's Figure 3 underneath the reference numerals 302, 304, and 306 and such can be shared between users, such as John and Carol in Figure 4.* Simultaneously, system administrators are managing the safes, containing the profiles, but never obtain the underlying data of the profile. Moreover, neither reference teaches multiple such profiles for each user different from one another that are shared with multiple other users.

The Applicant does not dispute that Van Dyke teaches granting control of access rights to administrators. The Applicant, further, does not dispute that the prior art is replete with instances of usage where administrators have various access rights granted. However, to suggest that because Van Dyke broadly teaches granting of administrator rights it somehow, in combination with Chang, renders the claims obvious, is to over-generalize or over simplify the relationship of the claim terms.

Again, claim 1 precisely requires administrators to have "access rights" granted to "a vault." At the same time, the vault contains "multiple user objects for multiple users," in turn, each user object "having a corresponding safe object." To these safe objects, "multiple

different profiles" thereof are "accessed and administered exclusively by a single one of the multiple users at the exclusion of the administrator." Ultimately, each of the multiple different profiles including digital information are "operable to be shared with other of the multiple users having other multiple different profiles accessible and administered exclusively by the other of the multiple users." "Sharing" [of profiles] then "occurs exclusively upon initiation by the single one of the multiple users."

In other words, claim 1 requires a precise interaction of rights between a user, an administrator and still other users at a time when users share, to the exclusion of the administrator, underlying data of profiles. It also requires them in a context related to a complex compilation of a vault, a user object, a safe object, and multiple different profiles of underlying digital information. Van Dyke, at best, grants access rights to another party to receive e-mail, for example. Chang, at best, stores a single profile (e.g., access list, password) of a system administrator in a repository in an administrator server, for example. In turn, the Applicant submits that rejecting these precise claims as obvious in view of Van Dyke and Chang's broad teaching is akin to arguing that a broad genus anticipates or renders obvious a definitively more narrow species.

In contrast, the law has long provided, a "prior art reference that discloses a genus still does not inherently disclose all species within that broad category." *Metabolite Laboratories, Inc. V. Laboratory Corp. of America Holdings*, 71 USPQ2d 1081, 1091 (Fed. Cir. 2004)(The court also quoted from *Corning Glass Works v. Sumitomo Elec. USA, Inc.*, 868 F.2d 1251, 1262 [9 USPQ2d 1962] (Fed. Cir. 1989)("Under [defendant's] theory, a claim to a genus would inherently disclose all species. We find [this] argument wholly meritless [sic]. . . .").

The Applicant respectfully reminds the Examiner that it is impermissible to utilize hindsight reconstruction when examining the claims. The proper test of obviousness is

whether the differences between the invention and the prior art are such that "the subject matter as a whole would have been obvious at the time the invention was made" to a person skilled in the art. *Stratoflex Inc. V. Aeroquip Corp.*, 713 F.2d 1530, 1538 (Fed. Cir. 1983)(Underlining added). Bear in mind, the Applicant originally filed for patent protection on September 27, 2000. It is now nearly five full years after filing. The Applicant also reminds the Examiner of caution expressed by the Court of Appeals for the Federal Circuit that "[d]etermination of obviousness can not be based on the hindsight combination of components selectively culled from the prior art to fit the parameters of the [] invention." *ATD Corp. v. Lydall, Inc.*, 159 f.3d 534, 536 (Fed. Cir. 1998).

Still further, each of the claims distinguish themselves over the art of record for at least the following reasons:

**Claim 1** requires a database having a vault for storing multiple users objects of multiple users. In turn, the user objects have safe objects which contain "multiple different profiles" of the users that are accessed and administered exclusively by the users, at the exclusion of the system administrator, and are able to be shared with one another. Chang, however, only describes single profiles of administrators (e.g., access list, password) that are never shared amongst other administrators. Van Dyke, on the other hand, never mentions vaults, user objects, safe objects or profiles. Van Dyke also avoids describing the sharing of underlying data between users. At best, Van Dyke teaches the granting of control access rights to other parties, but never access to underlying data. To the extent Van Dyke teaches granting of control access rights to a user for the sending/receiving email of another user (*col. 9, ll. 60-64*), e-mails are not "profiles" as described by the Applicant. E-mails are also not stored in safe objects of a vault. Further, if a party composes a new email on behalf of another party, this is not the sharing of multiple different profiles stored in a safe. Rather, it is the composition of original thought in an e-mail. On the other hand, if a party receives

an e-mail on behalf of another party, this is not the sharing or exchange of multiple different profiles stored in the same vault between users. It is simply receiving original thought composed by another user. Clearly, the claims are not so broad as to read on or remove from the public domain the sending and receiving e-mails between parties. The Applicant does not then understand how Chang and Van Dyke can possibly render the claims obvious;

**Claim 90** requires a vault "having access rights granted to one or more system administrators including management of the one or more safes of digital identities of one or more accounts of end users" and "one or more safes of digital identities" in the vault "having access rights granted exclusively to the end users via the one or more accounts including the exclusion of access rights of the one or more system administrators." In other words, without restricting the claim scope beyond the words expressly recited, administrators have access rights to vaults and to the management of the accounts of end users. End-users have exclusive access rights to their digital identities in the vault, yet obtained these rights via their accounts, in turn, managed by the administrator. In still other words, end users have access to the substance of underlying data of their digital identities while administrators give the end users their ability to get to the substance. Neither Chang nor Van Dyke teach such a system. Further, the claim requires "sharing" of the "multiple profiles" of the multiple end users. In contrast, Chang never mentions sharing of profiles, let alone multiple profiles of multiple users. Van Dyke does not supply the missing teaching because it simply grants control of access rights, but never grants access of underlying data to anyone. In fact, Van Dyke especially defined the grant of control access rights and intentionally limited it from including granting of access to underlying data. *See, e.g., col. 5, ll. 41-44;* and

**Claim 98** requires access rights to the vault be given to system administrators while access rights to the multiple digital identity profiles, stored in the vault, be given to end users exclusively. Also, the claim requires "sharing" of the multiple profiles of the multiple end

users to the exclusion of the system administrator. In contrast, Chang never mentions sharing of profiles, let alone multiple profiles of multiple users. Van Dyke does not supply the missing teaching because it simply grants control of access rights, but never grants access of underlying data to anyone. Further, claim 98 requires the location of the end users to be remote from the vault. Chang, conversely, teaches all operations at "a central location." On the other hand, Van Dyke nowhere mentions complexities of 1) safes in vaults; 2) vaults including three layers, especially an access protocol layer, an identity server layer and an identity manager layer; 3) digital identity profiles; and 4) the relationship of administrators and end users to the safes, vaults and profiles. Reconsideration is, thus, respectfully requested.

The entirety of the dependent claims are submitted as being patentable because of their dependence on one of claims 1, 90 or 98 discussed above. In instances where the dependent claims have been amended, these primarily relate to antecedent basis issues. Of course, additional reasons of patentability can be given but are being held in abeyance in anticipation of a Notice of Allowance.

The Applicant submits all claims are in a condition for allowance and requests a timely Notice of Allowance be issued for same. ***To the extent any fees are due beyond those expressly authorized in the accompanying transmittal forms for the Request for Continued Examination, the undersigned authorizes the deduction from Deposit Account No. 11-0978.*** None are believed due, however, because the Applicant has previously paid the RCE filing fee under 37 C.F.R. §1.17(e). The Applicant has also paid for a two-month time extension.

***Finally, the Applicant requests a change in the attorney document number of***

***record. Namely, please replace 1909.2.74A with 1363-006.*** The docket number changed when the new Power of Attorney (POA) went into effect.

Respectfully submitted,

**KING & SCHICKLI, PLLC**

Michael T. Sanderson
Registration No, 43,082

247 North Broadway
Lexington, Kentucky 40507
Phone: (859) 252-0889
Fax: (859) 252-0779

Certificate of Mailing
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: MAIL STOP RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450
on Sept. 6 2005
Date 9-6-05 by Carolina Perdomo